SANS

Analyst Program

Whitepaper

A SANS 2021 Report: Making Revolutionary Gains in Security on Your Endpoints

Written by **John Pescatore**

September 2021

KEYSIGHT TECHNOLOGIES

Executive Summary

There is an internet security truism that says, “The internet is actually pretty secure—it is all those vulnerable endpoints that are the problems.” Despite years of increased spending on endpoint security, more than 70% of successful attacks still involve compromised endpoints. To keep information, customers, and businesses safe, endpoint security needs to improve dramatically.

Securing user devices is a complex problem, but it is not an unsolvable problem. Many enterprises have made dramatic improvements in meeting business demands for user applications and internet access, while successfully avoiding or mitigating business risks. However, no single solution or product is the answer to every organization’s endpoint security problem.

This SANS whitepaper details a process to evaluate your existing endpoint security strategy and move to security controls and processes that increase current levels of protection and provide a platform for staying ahead of evolving threats. The key points include:

- Undergo a realistic evaluation of your starting point across people, process, security controls, and technology.
- Define the needed levels of endpoint security based on business-critical technology use, IT and security governance approaches, and threat patterns.
- Take advantage of “success factors” used by others to move to more effective and efficient endpoint protection.
- Define and collect metrics to evaluate progress and demonstrate gains to management.

Evolution of Enterprise Endpoints, Threats, and Security Controls

As computing platforms have evolved over the years, threats have evolved as well (see Figure 1). The increases in sophistication of threats drove reactive changes in the standard endpoint security software used to reduce the likelihood that threats would succeed and cause damage.

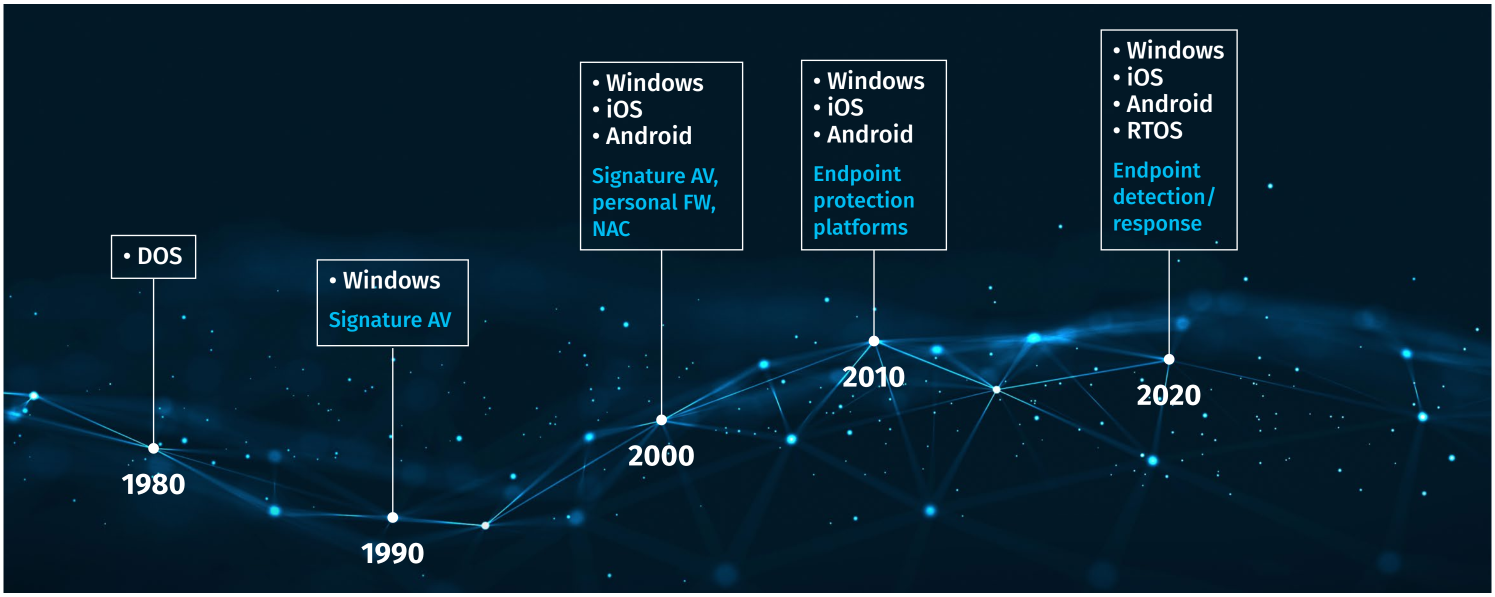


Figure 1. Evolution of Endpoints and Threats

It is important to note that most attacks take advantage of known vulnerabilities that haven't been patched or shielded. Essentially, secure hygiene around asset discovery/inventory, configuration management, patching, privilege management, and strong authentication raises the bar against all levels of attack. Moving to more proactive forms of endpoint protection addresses the remaining gaps.

The first virus to hit DOS PCs (Brain in 1987) prompted the development of signature-based anti-viral software, which became the baseline for tower-based Windows PCs that were usually behind network security devices such as firewalls on corporate networks.[1] As workforces became more mobile, laptops began to replace tower PCs. Laptops were commonly directly connected to the internet, outside of the protection of corporate firewalls. Personal firewall software was added to the endpoint security stack to reduce risk when mobile and network access control (NAC) software was used to assess a laptop's security state when returning to the corporate network.

Progression of New Threats

Each wave of new technology beings a predictable wave of vulnerabilities (some new, many old) and leads to a predictable progression of new threats:

- **Denial of service attacks happen first.** Attackers with even minimal skills can find ways to cause devices, applications, and services to crash, but usually in an unpredictable manner that doesn't support criminal or nation-state activity.
- **Simple malware insertion attacks follow.** More sophisticated attackers start to craft executables or scripts and use phishing attacks to get malicious payloads installed on endpoint targets.
- **Attacks use enhanced targeting and evasion to bypass standard protections.** High-end cybercriminals and nation-state attackers use sophisticated tools, tactics, techniques, and procedures to cause high levels of damage.

[1] www.cs.umd.edu/class/spring2018/cmsc414-0101/papers/3viruses.pdf

When Apple introduced the iPad and the iPhone, and later when Google first offered Android-based tablets and phones, user demand for BYOD skyrocketed. However, attacks were slow to succeed on those platforms for a variety of reasons. Over time, serious vulnerabilities in the mobile operating systems and processors used in device hardware enabled numerous sophisticated attacks against those devices.

Later, waves of movement to cloud-based applications and processing and the rise of corporate use of and reliance on IoT devices resulted in increased heterogeneity in devices (harder for IT operations to configure and manage securely) and an expanded attack surface (harder for cybersecurity teams to defend), which resulted in longer times to detect and mitigate attacks.

The SANS 2021 Endpoint Monitoring in a Dispersed Workforce Survey demonstrates the increasing level of endpoint heterogeneity, which IT operations is often unable to manage centrally (see Figure 2).[2]

The SANS 2021 Top New Attacks and Threat Report[3] projected the key "next wave" attacks that enterprises need to be prepared for:

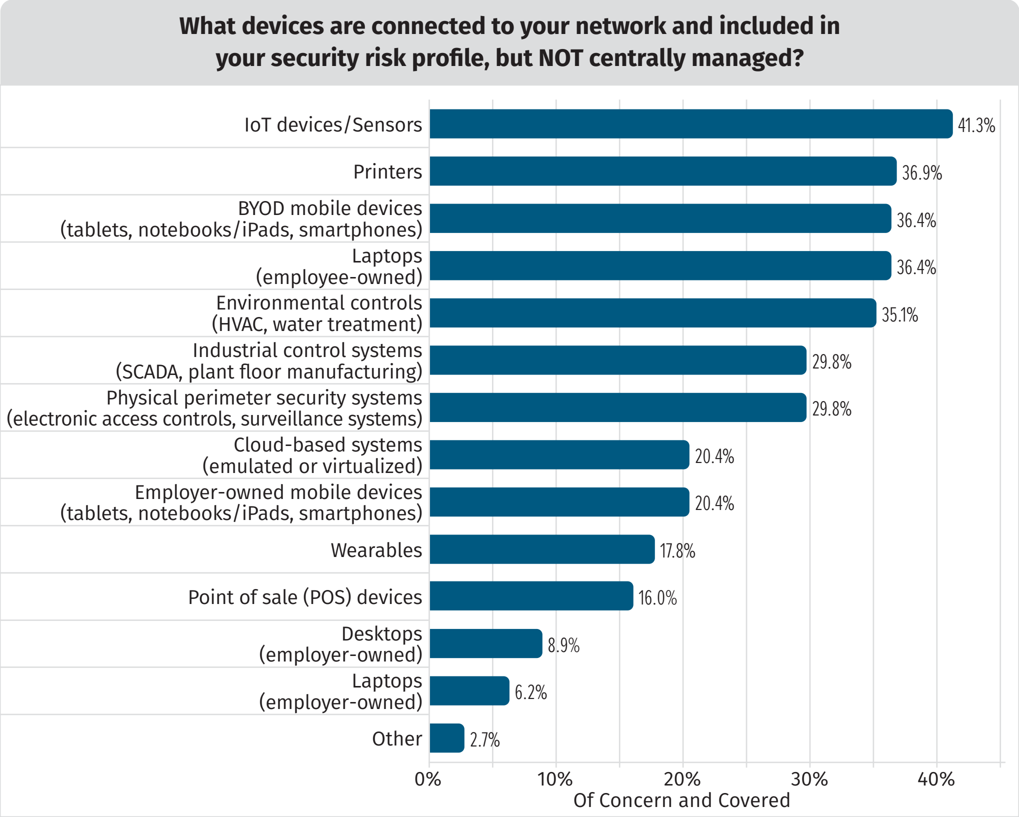


Figure 2. Endpoints Included in Security Risk Profiles but Not Centrally Managed

- **Software integrity attacks—**This is the broader class of attacks against applications that include what have been called "supply chain attacks," such as the SolarWinds compromise.
- **Improper session handling—**Mobile applications use software tokens to provide a reduced sign-on experience for users across complex mobile applications. This is often done insecurely, creating openings for attackers against mobile users.
- **Machine learning (ML) corruption/reverse engineering—**As enterprises increase use of ML-based security controls, attackers are developing techniques to evade or bypass detection.
- **Ransom/breachware—**Ransomware attacks are no longer just denial of service attacks. Data exfiltration is part of most ransomware attacks, increasing damage levels while simultaneously creating new opportunities for detection.

[2] "SANS 2021 Endpoint Monitoring in a Dispersed Workforce Survey," March 2021, www.sans.org/white-papers/40200/, p. 5, Figure 5. [Registration required.]

[3] "SANS 2021 Top New Attacks and Threat Report," August 2021, www.sans.org/white-papers/40405/, p. 5. [Registration required.]

The takeaways from these trends:

- Business demand for work from anywhere, mobile applications, and widespread use of cloud services has increased the diversity of devices, operating systems, and applications that must be protected. This has made it harder for IT operations to control and patch configurations, which increases vulnerability exposures.
- To decrease the likelihood of successful attacks—and decrease time to detect and mitigate attacks that do succeed—security architectures, processes, and controls must reduce reliance on static and reactive approaches.
- No level of protection has even been or ever will be perfect. Real gains in reducing successful attacks must be accompanied by reducing time to detect attacks that do get through while maintaining (or improving) time to restore business operations.
- Every wave of technology brings new threats, but also creates opportunity for new security approaches to be baked into the PCs, servers, services, and devices used.

Critical Endpoint Security Gaps

To deal with the risk raised by these trends, enterprises need to assess their current state of security, identify the highest risk gaps, and develop and deploy effective and efficient architectures, processes, and controls to close those gaps. Using an industry-accepted security framework is the best starting point for such a gap assessment.

The widely used NIST Cybersecurity Framework has expanded on the concept with five core functions (see Figure 3).[4]

- **Identify—**Maintain accurate and current knowledge of threats, high-value assets, and vulnerability and configuration status of all endpoints and services, and ensure response plans are in place.
- **Protect—**Avoid or limit attack damage by securely configuring and maintaining all endpoints and services and deploying security controls to minimize attack surface and shield vulnerabilities that cannot be avoided.
- **Detect—**Rapidly detect and profile attacks that reach endpoint devices and communicate details to security operations analysts and applications.
- **Respond—**Minimize damage and disruption by quickly taking action to stop the bleeding and establish a trustable baseline for restoration of services.
- **Recover—**Support rapid restoration of business services and data through temporary and permanent means. Take advantage of knowledge gained to improve overall level of preparation and protection against similar incidents in the future.

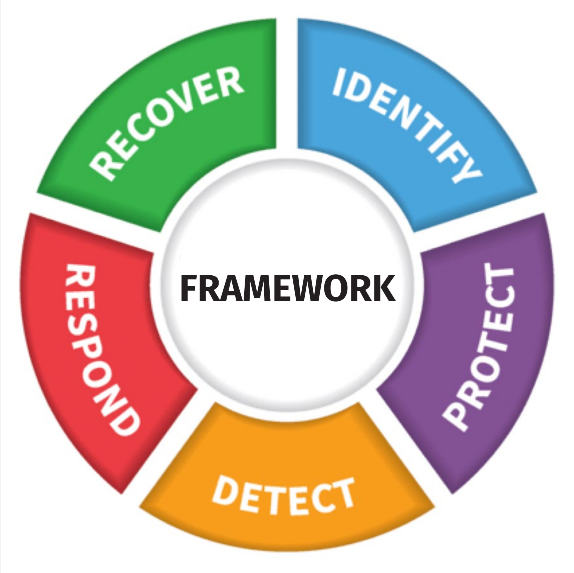


Figure 3. NIST Cybersecurity Framework Functions

[4] https://doi.org/10.6028/NIST.CSWP.04162018

For the purposes of this paper, we'll use a slightly consolidated set of functions. The automotive industry has reduced car crash fatalities through the years by looking at safety in three dimensions:

- **Before the crash—**Better visibility for drivers and improvements in automated warnings of dangerous conditions and automated remediation (anti-lock brakes, collision avoidance braking, etc.)
- **During the crash—**Chassis design to absorb impact forces before they reach the driver and passengers
- **After the crash—**Data capture and alerting capabilities to reduce time for appropriate medical assistance to arrive

The cybersecurity equivalents are before the incident, during the incident, and after the incident. Defining, monitoring, and tracking metrics for each phase are critical for both determining the effectiveness and efficiency of endpoint protection and for demonstrating progress to management to justify future tactics and strategies.

Before the incident. Assure that all endpoint and network configurations are as secure as possible, segmentation is enforced, and attack apertures are minimized (see Table 1).

During the incident. Detect malicious activity quickly, and take rapid action to minimize damage and minimize disruption of mitigation (see Table 2).

After the incident. Minimize time to restore full business operations, remedy/mitigate failure modes, and update defenses to reduce future risk (see Table 3).

Across these phases, three common high-level metrics emerge:

- Time to detect
- Time to mitigate
- Time to restore

Table 1. Before the Incident

Before the Incident Gaps	Metrics
Insecure configuration	% compliant to configuration benchmark
Missing patches/mitigations	Time to patch, % up to date
Overprivileged applications	% privileges above user, % ghost accounts
Zero day risk	Time to detect, time to mitigate
Unknown device/rogue IT	Time to detect, % accurate asset Inventory

Table 2. During the Incident

During the Incident Gaps	Metrics
Reliance on static controls	Time to detect, time to mitigate
Privilege escalation	Time to detect, time to mitigate
Lateral movement	Time to detect, time to mitigate
Lack of visibility	Multiple methods in use coverage

Table 3. After the Incident

After the Incident Gaps	Metrics
Insufficient backup/COOP	% critical information and executables securely backed up
Long/disruptive restoration	Date of last test, time to restore
Incomplete restoration	Multiple methods in use, time to restore
Repetitive damage	Restore playbook update frequency

These are three standard metrics all security operations teams need to be tracking. They can be further broken down into business- and security architecture-specific metrics that will differ by organization.

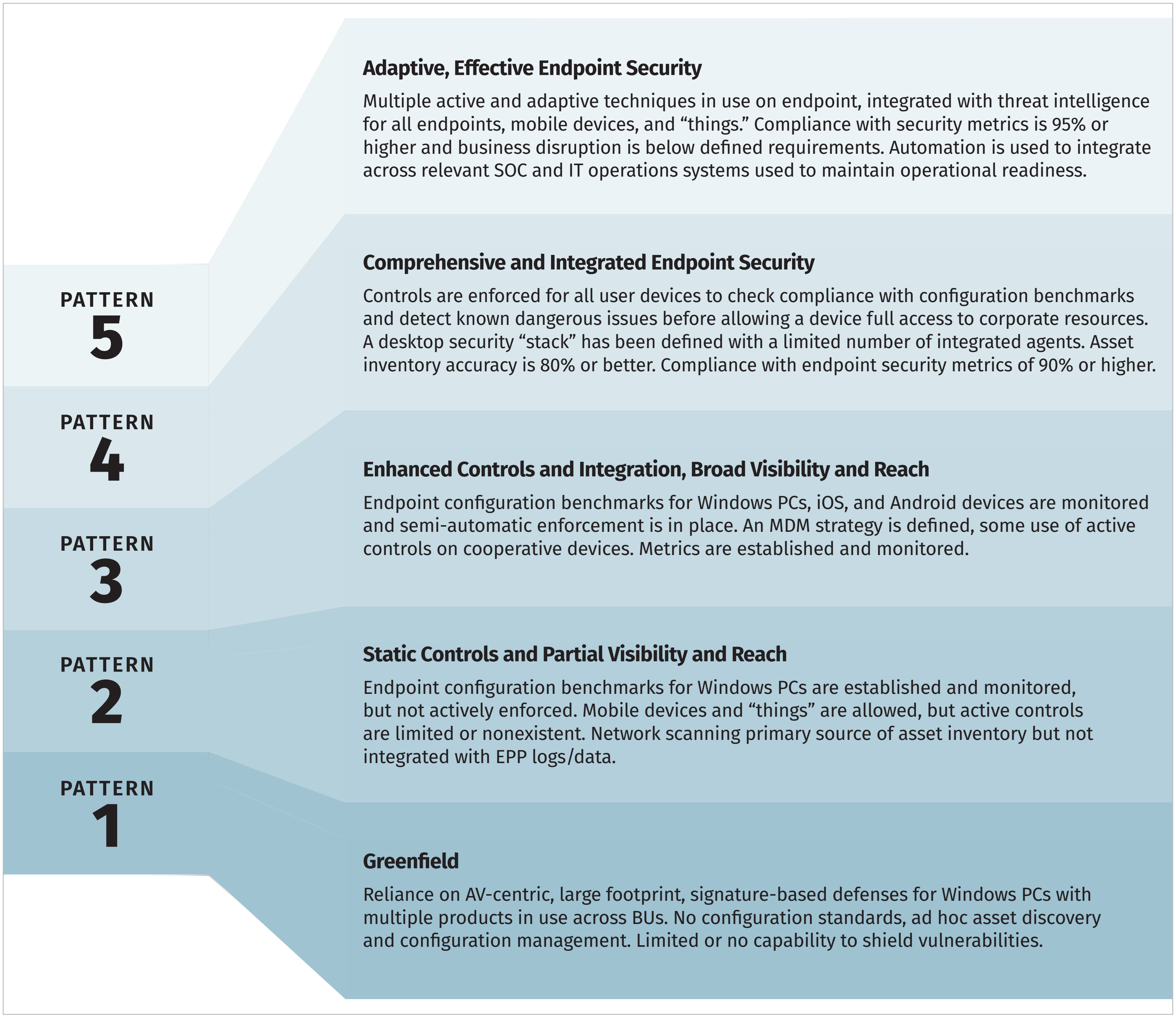
A gap analysis should be performed between the current state of those metrics and the necessary state driven by business needs. The gaps discovered should be prioritized by their impact on business needs and risks. A meaningful gap analysis must start from a definition of the needed state and should be based on a realistic assessment of the current effectiveness and efficiency of endpoint security.

The next step is to define strategies, processes, and architecture changes to close as many gaps as possible. Simply adding more layers of controls will be neither effective nor efficient, and so fixes for each gap should be looked at independently. The only long-term, effective approach is to look for integrated approaches that ultimately will demonstrate real improvement across all three major metrics.

[5] "Building an Information Security Program Post-Breach Part III," www.sans.org/blog/building-an-information-security-program-post-breach-part-iii/

Revolutionary Steps to Close Gaps in Endpoint Protection

One way SANS has found useful to close these gaps is to use a “success patterns” model that shows the common levels of risk reductions other enterprises have been able to achieve over time and what strategies, processes, and architectures they had in common during their progress. This approach is similar to Maturity Models but focuses more on quantitative operation improvement vs. subjective estimates of maturity.[6] Figure 4 illustrates the Endpoint Security Success Pattern Model.



PATTERN 5

Adaptive, Effective Endpoint Security

Multiple active and adaptive techniques in use on endpoint, integrated with threat intelligence for all endpoints, mobile devices, and “things.” Compliance with security metrics is 95% or higher and business disruption is below defined requirements. Automation is used to integrate across relevant SOC and IT operations systems used to maintain operational readiness.

PATTERN 4

Comprehensive and Integrated Endpoint Security

Controls are enforced for all user devices to check compliance with configuration benchmarks and detect known dangerous issues before allowing a device full access to corporate resources. A desktop security “stack” has been defined with a limited number of integrated agents. Asset inventory accuracy is 80% or better. Compliance with endpoint security metrics of 90% or higher.

PATTERN 3

Enhanced Controls and Integration, Broad Visibility and Reach

Endpoint configuration benchmarks for Windows PCs, iOS, and Android devices are monitored and semi-automatic enforcement is in place. An MDM strategy is defined, some use of active controls on cooperative devices. Metrics are established and monitored.

PATTERN 2

Static Controls and Partial Visibility and Reach

Endpoint configuration benchmarks for Windows PCs are established and monitored, but not actively enforced. Mobile devices and “things” are allowed, but active controls are limited or nonexistent. Network scanning primary source of asset inventory but not integrated with EPP logs/data.

PATTERN 1

Greenfield

Reliance on AV-centric, large footprint, signature-based defenses for Windows PCs with multiple products in use across BUs. No configuration standards, ad hoc asset discovery and configuration management. Limited or no capability to shield vulnerabilities.

Figure 4. Endpoint Security Success Patterns

[6] “Cybersecurity Capability Maturity Model,” www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

Pattern 5: Adaptive, Effective Endpoint Security

This is the level at which it becomes possible to deliver zero trust security. All connections to all corporate resources have NAC inspection and enforcement, with selective access levels for any devices judged to be compromised, noncompliant, or of unknown station, including IoT "things."

The endpoint security stack uses signature- and anomaly-based detection and other controls to reduce attack surface, and is integrated with threat intelligence information, access controls, and DNS/DHCP data and automation capabilities. Asset inventory completeness and accuracy is above 90% and compiled at least daily. Time to detect/mitigate/restore metrics are at values sufficient to meet business needs and are met more than 95% of the time. Business disruption due to cyberattacks is at an acceptable level to the business.

Pattern 4: Comprehensive and Integrated Endpoint Security

NACs are enforced for all user devices to check compliance with configuration benchmarks and detect known dangerous issues before allowing a device full access to corporate resources. A desktop security "stack" has been defined with a limited number of agents that are integrated. MDM has been extended to more active controls. Backups for data stored on mobile devices and "things" have been initiated. Asset inventory completeness and accuracy is above 80% and compiled at least weekly. Time to detect/mitigate/restore metrics are at values sufficient to meet business needs and are met more than 90% of the time.

Pattern 3: Enhanced Controls and Integration, Broad Visibility and Reach

Endpoint configuration benchmarks for Windows PCs, iOS, and Android devices are monitored with semi-automatic enforcement in place. EPP agents are supplemented with additional security agents for partial endpoint detection and response (EDR) capabilities. An MDM strategy is defined with some use of active controls on cooperative devices. Automated backup for internet-connected Windows PCs is established. Network scanning and endpoint agent logs are used for asset inventory with identification/classification. Monitoring of time to detect/mitigate/restore metrics are established, and values are sufficient to meet business needs are not yet met.

Pattern 2: Static Controls and Partial Visibility and Reach

Endpoint configuration benchmarks for Windows PCs are established and monitored, but not enforced. Endpoint protection platforms are in use for Windows PCs, but controls enabled are mostly static defenses. Mobile devices and "things" are allowed, but active controls are limited or nonexistent. Backups for Windows PCs are standardized but require domain login and don't include mobile devices. Network scanning is used for asset inventory and improved classification, but not integrated with EPP logs/data. Time to detect/mitigate/restore metrics are established but not tracked.

Pattern 1: Greenfield

At this level, there is no use of endpoint configuration benchmarks. Instead, there is a reliance on AV-centric, large footprint, signature-based defenses for Windows PCs with multiple products in use across BUs. Phones, tablets, and "things" are typically prohibited but not detected when used. Backups are manual or partial. Asset inventory depends on IT domains or sporadic network scans with limited or no automated identification/classification. No time to detect/mitigate/restore metrics.

Patterns 1–4 are typical starting points, and 4 and 5 are the ultimate goals. Success patterns generally involve moving from levels 1 and 2 to levels 3 or 4; or, for more advanced organizations, from level 4 to level 5. Making progress through the levels is not simply choosing and adding new security controls or even just defining new security processes. Movement upward invariably requires driving change: change in how endpoints are deployed and managed by IT operations, change in how employees use the devices, and change in the overall security architectures in use. The ability to demonstrate progress in key security metrics is an integral part of getting management backing for such change.

Driving Endpoint Security Change: Overcoming Obstacles

All enterprises are different, and the optimal strategy for reaching needed endpoint security levels will be different, as well. However, key patterns in overcoming typical obstacles and meeting business needs for endpoint security and safety have emerged over time. The following sections summarize those actions for typical starting and goal patterns.

Pattern 1 to Pattern 2: Leaving Chaos

The key first step in moving upward from the Greenfield pattern (in maturity model constructs this is often called the "chaotic" level) is increasing the completeness and accuracy of your endpoint asset inventory, independently of the means that IT operations uses. The use of EPP or other security agent reporting is not sufficient because rogue IT and unsupported devices will not be discovered. Network scanning is typically added.

Discovery of devices is important, but risk assessment requires knowing what devices are vulnerable, which requires that baseline configurations be defined and that vulnerability assessment against those baselines be part of the asset discovery process. Repeatable processes are defined to reach this level and utilize tools to automate repetitive functions to increase efficiency and accuracy.

Static EPP platforms may still be used at this level but, where possible, product choices should be standardized and chosen for manageability and ability to be integrated with other security controls. Employee awareness training should be ongoing, and security operations skills gaps should be identified.

This is an important time to get buy-in and cooperation from IT operations, because typically they are responsible for deploying and managing the configuration of endpoints. The focus here is on established, repeatable processes that will start out being labor-intensive but will provide a stable starting point to higher levels of protection that will increase effectiveness and support increased efficiency.

Pattern 2 to Pattern 3: Integration, Reducing Time to Detect and Time to Mitigate

To make this level of progress, static EPP platforms need to be replaced or augmented with more advanced capabilities, commonly called endpoint detection and response (EDR). The goal is to move beyond total dependence on reactive, signature-centric defenses and incorporate more advanced techniques that can detect potentially dangerous behavior or traffic, provide rapid alerting, and support semi-automatic response. Integrating both threat intelligence and vulnerability information is necessary here. Infrastructure control points such as DNS are used for early detection and disruption of attacks.

A strategy and/or playbook for securing mobile devices needs to be defined to include iOS and Android devices in the asset inventory and vulnerability assessment process. Network scanning and security endpoint agent reporting are integrated and used to identify/characterize the types of endpoints discovered. NAC support for segmented access is enabled.

Backups for Windows PCs and laptops are automated, but not regularly tested. Testing and simulation capabilities for new threats against existing security control baselines are evaluated and included in security plans.

Pattern 3 to Pattern 4: Reducing Risk, Automating More Alerting and Response

NAC enforcement is active for all endpoint connections to corporate resources, with enforcement enabled in addition to compliance reporting. A standard Windows endpoint security "stack" has been selected to deliver integrated EDR, NAC, and mitigation services.

Mobile devices are included in backup strategies and NAC services. Regular endpoint vulnerability assessment includes mobile devices and is done proactively as threat intelligence requires. A strategy for including IoT "things" is defined and is part of IT/OT integration plans.

Security operations skill levels are again evaluated, because movement upward from this pattern requires advanced skills to avoid the need for increased security headcount. SOC tools are enhanced to integrate with identity management and DNS information and controls. Testing and simulation systems or tools are procured and integrated into the SOC for assuring that endpoint protection metrics will be maintained against emerging threats.

Pattern 4 to Pattern 5: Increasing Efficiency, Adaptability, Speed, and Accuracy of Action

The top pattern of endpoint security essentially delivers proactive protection of all endpoints at a service level that meets business needs without disrupting business operations.

The endpoint security stack has been augmented with processes and tools to enable increased automated response or faster semiautomatic response by skilled analysts. Endpoint configurations are locked down sufficiently, and NAC functions are implemented to support zero trust access and segmentation across all devices and all corporate resources. Playbooks are defined and regularly updated, SOAR tools can be used to enable lesser-skilled analysts to work from prioritized alert lists and take rapid action to avoid or reduce damage.

Backup strategies are automated across all endpoints and restoration is tested periodically. Endpoint security and backup/recovery services work independently of employee location and "work from home" drills are performed at least semiannually to ensure effectiveness. Critical IoT devices are included in backup and recovery processes.

Real movement to higher pattern levels will result in improvements in one or more of the security metrics discussed earlier, providing data to justify the return on investment in enhancing security controls, processes, and skills. However, this requires designing approaches to collect the appropriate information in order to calculate and monitor metric values. Movement to higher level patterns also includes this effort.

Summary

Back in 2002, as part of Microsoft's efforts to improve Windows security, Microsoft CEO Steve Ballmer noted, "About 20% of the bugs causes 80% of all errors, and—this is stunning to me—1% of bugs caused half of all errors."[7] Almost 20 years later, these ratios hold true overall for endpoint security—80% of successful attacks exploit the same well-known problems that represent roughly 20% of all vulnerabilities. Software flaws are a big part of the problem, but configuration mistakes and rogue IT often expose gaps in security processes and controls that also enable attackers to succeed.

Enterprises that have reduced business damage by improving endpoint security have done so by first deploying more effective and efficient approaches to reducing exposure to common attack vectors and then building advanced capabilities on top of that foundation. The patterns of success described show that integration across threat information, infrastructure data sources and controls, and security systems and controls are key to making meaningful improvements in business-relevant security metrics.

This approach supports not only higher levels of accuracy and speed in identifying and mitigating threats, but also enables better prioritization and allocation of resources to make sure that that one vulnerability that could cause the 50% of damage that Ballmer found so stunning is eliminated. Making these revolutionary changes in endpoint security processes, controls, and metrics will lead to demonstrable improvements in both the effectiveness and efficiency of endpoint security expenditures.

[7] "Microsoft's CEO: 80-20 Rule Applies To Bugs, Not Just Features," www.crn.com/news/security/18821726/microsofts-ceo-80-20-rule-applies-to-bugs-not-just-features.htm

About the Author

John Pescatore joined SANS as director of emerging security trends in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems and “the occasional ballistic armor installation.” John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008, and is an NSA-certified cryptologic engineer.

Sponsor

SANS would like to thank this paper’s sponsor:

KEYSIGHT
TECHNOLOGIES